SecureMethods Embedded PKI™ the Next Generation Security Infrastructure

Abstract

Traditional information security approaches such as passwords and user IDs are of limited effectiveness in many organizations because of inherent weaknesses and reliance on the human factor to make them work. Attempts to overcome the limitations of these approaches using encryption-only solutions and Public Key Infrastructures based on low assurance products and architectures have seen limited success because they are deployed using a session management approach, instead of a more granular transaction-oriented approach. VPN schemes like SSL are hard to implement and require complex integration with a variety of web services and application servers – and they still do not offer the necessary level of assurance.

What is needed is a new generation of security infrastructure that supports transaction security as well as encrypted sessions. This functionality should be transparent to users thereby significantly reducing the security breaches caused by the human factor. This approach must overcome the limitations of current PKI and SSL implementations and provide an unprecedented level of security, building in the ability to address variable assurance and multi-level security concerns within a single product and across multiple organizations.

SecureMethods has developed such a Next Generation Security architecture, designed specifically to address these issues. The SecureMethods architecture seamlessly integrates with new and existing applications and provides a wide range of security features, including embedded PKI, encryption, access control, embedded digital signatures and per transaction transparent auditing in one product.

The SecureMethods architecture consists of two components: a gateway appliance component (SM Gateway™) and a client component (SM Client™). With these components and Embedded PKI™ technology, it protects data against the basic threats of disclosure, forgery, corruption and repudiation. It uses public key cryptographic schemes, strong authentication, digital signatures and role-based authorization to provide a high level of security for transactions and stored data.

SM Gateway with its Embedded PKI technology provides variable assurance protection for existing application servers and databases with no modifications to the servers or the user interface. This security extends to client access across LAN, WAN, and wireless networks. SM Gateway decrypts, verifies, and stores all inbound submissions and requests, and encrypts and signs outbound responses. It performs all authorization checking by comparing the originator's signature with a system resource access control matrix to verify the validity of the requested submission or retrieval operation based upon resource compartment and user role. All transactions are authorized and audited by SM Gateway, providing a single point of audit and security administration.

SM Client is a freely available software module that operates with industry standard web browsers and terminal interfaces to offer transparent digital signature and audit services for web and terminal based applications. SM Client also provides users the ability to encrypt and/or digitally sign desktop files for protected storage or transmission. Files may be signed for general receipt as well as encrypted only for designated individuals to decrypt and access the protected content.

Each user, “internal” or “external,” must be issued credentials in the form of X.509 certificates through a Certificate Authority (CA). SM Gateway and SM Client seamlessly use these credentials that may be stored in a local database or LDAP accessible directories.

Role-based authorization using digital signatures provides single sign-on with strong authentication capabilities for users. The user accesses the private key once and the embedded security in SM Client provides a digital signature to SM Gateway for authorization. The SM Gateway access control matrix

supports compartmentalized access at up to TS/SCI and in turn facilitates inter-organizational data sharing.

The SecureMethods architecture with its Embedded PKI™ technology offers a unique security solution that facilitates rapid deployment in any environment. Through implementation of the SecureMethods architecture and handling of secure transactions, SM Gateway can securely process data that has been encrypted, digitally signed, and even biometrically protected. Already deployed and proven in a variety of sensitive environments, SM Gateway can be configured and installed on a turnkey basis to provide hardened security for any network applications.